Centralized and Epidemic Dissemination of Security Patches

Kundan Kandhway
TCS Innovation Labs,
IIT Madras Research Park,
Chennai, India 600113.
Email: kundan.kandhway@tcs.com, kundan@iisc.ac.in

***Abstract*—We study optimal distribution of security patches in a network of devices where the distribution server can jointly decide (i) the intensity of patch distribution, and (ii) the optimal stopping time, to minimize it's cost function. In our model, peer-to-peer contacts between the network nodes aid in epidemic patch distribution in addition to direct patching by the central server. Once the server stops, patches are only disseminated through epidemic spreading by peer-to-peer contacts between the nodes in the network. We formulate the optimization problem as a free terminal time optimal control problem and use Pontryagin's Minimum Principle to obtain the solution. We find the optimal strategy to be considerably more effective than heuristic strategies. Our results show that, as the peer-to-peer patch dissemination between nodes in the network becomes more viral, both optimal server cost and optimal stopping time of the server decreases reflecting reduced workload of the server.**

I. Introduction

Malicious codes and worms pose significant threat to proper functioning of a network. Upon detection of a malicious code, security patches and software updates are generated and distributed among the devices (nodes) in the network to plug the vulnerabilities which the malware may exploit. Distribution of updates and patches exhausts resources—bandwidth, power etc.—at the server which motivates the need of optimal strategy for patch dissemination.

In this paper, we consider the problem of distributing security patches in a network of devices. In contrast to the traditional systems, where patches are only distributed by a central server, the proposed system is simultaneously aided by epidemic patch distribution between the nodes in the network using peer-to-peer contacts among the nodes. Based on an optimal control formulation, the central server decides the intensity of patch distribution to the nodes in the network, and the optimal time till which the patch is distributed. After the server stops, epidemic spreading patches the leftover vulnerable nodes.

Related works: Researchers have studied patch distribution in networks employing peer-to-peer dissemination models. Authors in [1] and [2] studied epidemic patch distribution without any control in the system. The work in [3] used optimal control to counter worm epidemics, but linearized the system which is inaccurate for late time behavior modeling of the system. Works in [4] and [5] made use of optimal control for patch distribution but considered the terminal time to be fixed and given. We formulate the problem where terminal time is also an optimization variable. Unlike previous works, in our model, once the central server stops the patch distribution, peer-to-peer dissemination still continues; leading to further spread of the security patches. The work in [6] studied message dissemination in vehicular networks but with a linear cost, while works in [7], [8] and [9] formulated optimal campaigning strategies in social networks as fixed time horizon optimal control problems.

A major difference in this work compared to the previous literature discussed above is that the previous literature formulates the dissemination problem as a fixed time horizon optimization problem; in contrast, our formulation has a free terminal time. In other words, the stopping time is an optimization variable too. It is possible to achieve further resource savings if the server is allowed to decide the optimal time horizon during which the patch will be distributed. After the specified time is crossed the dissemination is left entirely on the epidemic dynamics between the nodes which will patch the remaining nodes.

Contributions: In this paper we formulate a free terminal time optimal control problem to determine the optimal stopping time and optimal strategy for patch distribution which minimizes the cost from the server's perspective. We use Pontryagin's Minimum Principle to set up the optimality system which is solved numerically. We discuss how to solve the free terminal time boundary value problem obtained by the application of the Pontryagin's Minimum Principle, using readily available fixed terminal point boundary value problem solvers. We demonstrate the effectiveness of the optimal strategy over the heuristic strategies.

Our results reveal that server cost decreases as the peer-to-peer patch distribution becomes more viral, either by increasing peer-to-peer spreading rate, or by keeping the spreaders active for a longer duration of time. The active nodes then enter passive state where they stop patch dissemination. Similar trend is seen in the optimal stopping time—it reduces as the epidemic patch distribution becomes more viral.

II. System Model and Problem Formulation

The aim is to distribute software patches and updates in a network with N nodes using a central server. In addition to distribution by the central server, the patched network

nodes disseminate the security patches to the unpatched nodes using epidemic spreading (leveraging the peer-to-peer contact between the nodes). The central server wants to minimize its distribution cost—incurred due to use of bandwidth, power, etc.—by selecting optimal intensity of patching and an appropriate stopping time. After the server stops, peer-to-peer dissemination of security patches continues to patch the unpatched (leftover) nodes.

A. Patch Dissemination Model

A node in the network is divided into three classes, (i) susceptible (unpatched), (ii) patched and actively spreading, and, (ii) patched and passive. There numbers at time t is denoted by $S(t), A(t)$, and $P(t)$ respectively. Note that, $S(t) + A(t) + P(t) = N$. We denote the fraction of susceptible, active and passive nodes by $s(t), a(t)$, and $p(t)$ with $s(t) + a(t) + p(t) = 1$. As mentioned before, patching takes place through two mechanisms, peer-to-peer contact between nodes and direct contact with server.

We first explain the peer-to-peer mechanism of patch dissemination. A node which is already patched, makes B communication attempts per unit time by scanning from the space of valid addresses, to transfer the patch to a susceptible node. Let $1/\hat{\beta}$ be the average length of time it takes to patch a node due to peer-to-peer contact (which may depend on variable factors such as bandwidth availability at the susceptible/active node, workload at susceptible/active node etc.) In the fluid model, the increase in number of patched nodes (as $N \to \infty$) per unit time is then given by $B\hat{\beta}A(t)(S(t)/N)$, where $S(t)/N$ is the probability of encountering a susceptible node during the random scan (similar arguments have been used in previous studies such as [2]). Patch dissemination consumes resources at the node, so we allow the user of the node to switch off the dissemination after a random time which is exponentially distributed with mean $1/\gamma$ where γ is the passivity rate. At this point the node enters the passive class from the active class. Such a system dynamics leads us to the epidemic of type susceptible-infected-recovered (SIR) which is captured by the following system of ordinary differential equations (ODEs) [10]:

$$\begin{aligned} \dot{s}(t) &= -\beta s(t)a(t), \\ \dot{a}(t) &= \beta s(t)a(t) - \gamma a(t), \\ \dot{p}(t) &= \gamma a(t). \end{aligned}$$

Here dot represents time derivative and $\beta = B\hat{\beta}$ is termed as peer-to-peer spreading rate. Since $\dot{s}(t) + \dot{a}(t) + \dot{p}(t) = 0$, only two equations are sufficient to capture the dynamics of the system.

Server disseminates the patches as follows. Let the average length of time required to patch a node from the server be $1/\hat{\alpha}$ (which might depend on factors such as server workload due to other tasks, bandwidth limitations at server and/or susceptible nodes etc). Let at time t, server makes $Q(t)$ communication attempts per unit time to transfer the patch by randomly scanning the nodes from the space of all valid addresses. We define $u(t) = \hat{\alpha}Q(t)$ as the control signal at time t, with $u_{min} \leq u(t) \leq u_{max}$, and call it the intensity of patch distribution by the server. Practical considerations will impose such a restriction on the control signal. Thus in the fluid model, the increase in the number of patched node due to server activity is given by $u(t)s(t)$, where $s(t)$ is the probability that server encounters a susceptible node during the random scan.

For the controlled system (where both peer-to-peer and server patching is active), the system dynamics is governed by the following ODEs:

$$\begin{aligned} \dot{s}(t) &= -\beta s(t)a(t) - u(t)s(t), \\ \dot{a}(t) &= \beta s(t)a(t) - \gamma a(t) + u(t)s(t). \end{aligned}$$

The server computes the optimal value of the control signal, $u(t)$, along with the optimal server stopping time based on a cost function (to be discussed shortly). However, the population of active nodes keeps spreading the patches—till all the nodes reach the passive state—irrespective of the behavior of the server.

This work assumes that the nodes undergo homogeneous mixing to distribute patches. Previous studies have noted that this is a valid assumption in the following cases: (i) Wireless nodes randomly move in an area and exchange patches when in communication range [4]. (ii) In a wired network, from the space of valid IDs, active nodes generate addresses to transfer the patch to susceptible nodes [1], [2]. Authors in [11] have shown acceptable performance of homogeneous mixing criteria in certain networks.

B. Cost Functional

The cost functional (to be minimized by the server) is composed of two parts. The first part captures the penalty incurred by the server in distributing the patches, with penalty being zero when spreading intensity is zero. We assume the instantaneous cost of applying control $u(t)$ (incurred, for example, due to efforts made in scanning the address space) to be given by the function $g(u(t))$, with $g(0) = 0$ such that $g(.)$ is an increasing function of its argument. Also, if there are more susceptible nodes, the server has to spend more resources (e.g., bandwidth, power etc.) in serving them. Hence, the penalty due to patch distribution over the time horizon $0 \leq t \leq T$ is, $J_1 = \int_0^T g(u(t))s(t)dt$, where T is also an optimization variable.

The second part of the cost functional captures the reward due to patched nodes and is given by $J_2 = -\tilde{c}_1 a(T) - \tilde{c}_2 p(T)$, where T is the terminal time. Expressing in terms of only $s(.)$ and $a(.)$, we get, $J_2 = -c_1 a(T) + c_2 s(T)$, with $c_1 > 0, c_2 > 0$. Active nodes further patches susceptibles (after the server switches off), hence for practical systems $\tilde{c}_1 > \tilde{c}_2$. Once the server switches off, very small number of nodes actively spreading the patches is not desired as the patch distribution 'epidemic' may die out, hence the need of J_2. The cost functional to be minimized by the server is given by $J = J_1 + J_2$.

C. Optimal Control Problem

The best policy (patch distribution intensity, $u(t)$, and the stopping time, T) for the server which minimizes the cost functional, J, is not clear a priori; hence, the need of solving the following optimal control problem:

$$\begin{aligned}
\underset{u,T}{\text{minimize}}\ J &= \int_0^T g(u(t))s(t)dt - c_1 a(T) + c_2 s(T), \\
\text{subject to: } \dot{s}(t) &= -\beta s(t)a(t) - u(t)s(t), && \text{(1a)}\\
\dot{a}(t) &= \beta s(t)a(t) - \gamma a(t) + u(t)s(t), && \text{(1b)}\\
s(0) &= 1,\ \ i(0) = 0, && \text{(1c)}\\
u_{min} &\leq u(t) \leq u_{max},\ \forall t \in [0,T], && \text{(1d)}\\
& T \text{ is free.}
\end{aligned}$$

III. Solution to the Optimal Control Problem

We denote the optimal control by $u^*(t)$, state variables (at optimum) by, $s^*(t),\ a^*(t)$, costate variables (at optimum) by $\lambda_s^*(t),\ \lambda_a^*(t)$ and optimal stopping time by T^*. Application of the Pontryagin's Minimum Principle [12], [13], for free terminal time optimal control problems, leads us to the system of equations which the optimal system satisfies.

Hamiltonian: The Hamiltonian of the optimal control problem is defined as:

$$\begin{aligned}
&H(s(t), a(t), u(t), \lambda_s(t), \lambda_a(t), t)\\
=&g(u(t))s(t) + \lambda_s(t)\Big[-\beta s(t)a(t) - u(t)s(t)\Big]\\
&+ \lambda_a(t)\Big[\beta s(t)a(t) - \gamma a(t) + u(t)s(t)\Big].
\end{aligned}$$

State Equations: $\dot{s}^*(t)$ and $\dot{a}^*(t)$ is obtained by evaluating $\frac{\partial}{\partial \lambda_s(t)}H(.)$ and $\frac{\partial}{\partial \lambda_a(t)}H(.)$ respectively.

$$\begin{aligned}
\dot{s}^*(t) &= \frac{\partial}{\partial \lambda_s(t)}H\Big|_{\substack{s(t)=s^*(t),a(t)=a^*(t),u(t)=u^*(t),\\ \lambda_s(t)=\lambda_s^*(t),\lambda_a(t)=\lambda_a^*(t)}}\\
&= -\beta s^*(t)a^*(t) - u^*(t)s^*(t) && \text{(2)}\\
\dot{a}^*(t) &= \frac{\partial}{\partial \lambda_a(t)}H\Big|_{\substack{s(t)=s^*(t),a(t)=a^*(t),u(t)=u^*(t),\\ \lambda_s(t)=\lambda_s^*(t),\lambda_a(t)=\lambda_a^*(t)}}\\
&= \beta s^*(t)a^*(t) - \gamma a^*(t) + u^*(t)s^*(t), && \text{(3)}
\end{aligned}$$

with initial conditions,

$$s^*(0) = 1 \text{ and } a^*(0) = 0. \tag{4}$$

Costate Equations: The costate variables for the optimal system, $\dot{\lambda}_s^*(t)$ and $\dot{\lambda}_a^*(t)$ are obtained by evaluating $-\frac{\partial}{\partial s}H(.)$ and $-\frac{\partial}{\partial a}H(.)$ at the optimum.

$$\begin{aligned}
\dot{\lambda}_s^*(t) &= -\frac{\partial}{\partial s(t)}H\Big|_{\substack{s(t)=s^*(t),a(t)=a^*(t),u(t)=u^*(t),\\ \lambda_s(t)=\lambda_s^*(t),\lambda_a(t)=\lambda_a^*(t)}}\\
&= -g(u^*(t)) + \beta\lambda_s^*(t)a^*(t) + \lambda_s^*(t)u^*(t)\\
&\quad -\beta\lambda_a^*(t)a^*(t) - \lambda_a^*(t)u^*(t), && \text{(5)}\\
\dot{\lambda}_a^*(t) &= -\frac{\partial}{\partial a(t)}H\Big|_{\substack{s(t)=s^*(t),a(t)=a^*(t),u(t)=u^*(t),\\ \lambda_s(t)=\lambda_s^*(t),\lambda_a(t)=\lambda_a^*(t)}}\\
&= \beta\lambda_s^*(t)s^*(t) - \beta\lambda_a^*(t)s^*(t) + \gamma\lambda_a^*(t). && \text{(6)}
\end{aligned}$$

Hamiltonian Maximizing Condition: Evaluating,

$$\frac{\partial}{\partial u(t)}H\Big|_{\substack{s(t)=s^*(t),a(t)=a^*(t),u(t)=u^*(t),\\ \lambda_s(t)=\lambda_s^*(t),\lambda_a(t)=\lambda_a^*(t)}} = 0,$$

we obtain,

$$g'(u^*(t)) = \lambda_s^*(t) - \lambda_a^*(t).$$

Where $g'()$ is derivative of g with respect to its argument. This leads to,

$$u^*(t) = \begin{cases} u_{min} & \text{if } g'^{-1}(\lambda_s^*(t) - \lambda_a^*(t)) < u_{min},\\ g'^{-1}(\lambda_s^*(t) - \lambda_a^*(t)) & \text{if } u_{min} \leq g'^{-1}(\lambda_s^*(t) - \lambda_a^*(t)) \leq u_{max},\\ u_{max} & \text{if } g'^{-1}(\lambda_s^*(t) - \lambda_a^*(t)) > u_{max}, \end{cases}$$

$$\Rightarrow u^*(t) = \min\left\{\max\left\{g'^{-1}(\lambda_s^*(t) - \lambda_a^*(t)), u_{min}\right\}, u_{max}\right\}. \tag{7}$$

Transversality condition: For the free terminal time optimal control problem (1), the Transversality conditions are given by,

$$\begin{aligned}
&\lambda_s^*(T^*) = c_2, && \text{(8a)}\\
&\lambda_a^*(T^*) = -c_1, \text{ and} && \text{(8b)}\\
&g(u(T^*))s(T^*) + \lambda_s(T^*)\Big[-\beta s(T^*)a(T^*) - u(T^*)s(T^*)\Big]\\
&+\lambda_a(T^*)\Big[\beta s(T^*)a(T^*) - \gamma a(T^*) - u(T^*)s(T^*)\Big]\\
&+c_4 s(T^*) - c_3 i(T^*) = 0. && \text{(8c)}
\end{aligned}$$

A. Numerical Computation of the Solution

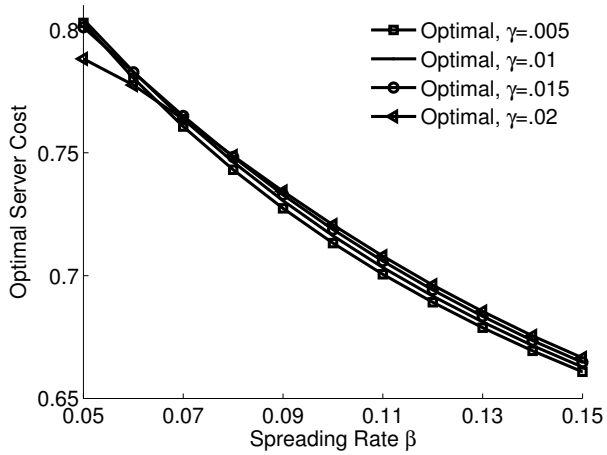
Solution to this problem confronts us with a boundary value problem with free terminal time. Most software packages only solve fixed end point boundary value problems, so we briefly discuss the methodology followed to obtain the solution.

Substituting $u^*(t)$ from (7) in (2), (3), (5) and (6), we get ODEs entirely in terms of state and costate variables. This system along with the initial conditions in (4) and the boundary conditions in (8a) and (8b) can be solved by a fixed end point boundary value solver[1] for a given value of terminal time T^*. We first determine two values of terminal time T_1^* and T_2^* where the values of left hand side (LHS) of (8c) are positive and negative respectively. Then using bisection method keep revising the estimate for T^* till the LHS of (8c) is below a predetermined threshold (close to zero). At this point all the requirements of Pontryagin's Minimum Principle are fulfilled; thus, $s^*, a^*, \lambda_s^*, \lambda_a^*$ and T^* are indeed solutions that can be substituted in (7) to obtain the optimal control, u^*.

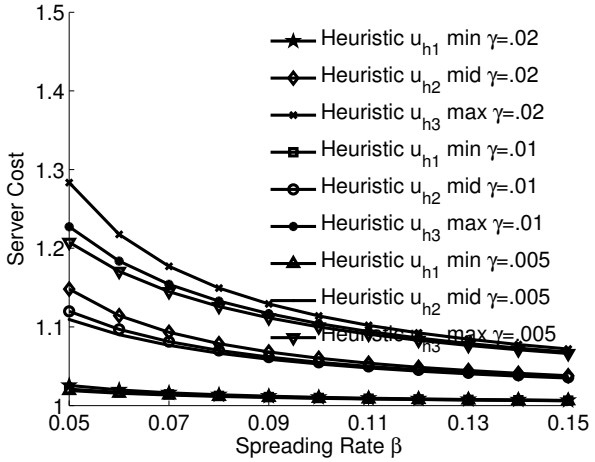
IV. Results

Unless otherwise noted, the values of parameters used in this section are: $c_1 = 3,\ c_2 = 1,\ u_{min} = 0.002$ and $u_{max} = 0.02$. We assume $g(u(t)) = c_3 u^2(t) + c_4 u(t)$, a quadratic function with $c_3 = 5,\ c_4 = 5$. Notice that $g(0) = 0$ as required. We keep revising our estimate of optimal stopping time T^* (as detailed in section III) until LHS of (8c) is below 10^{-5}.

[1]One may use Python's boundary value problem solver `scipy.integrate.solve_bvp()`, or MATLAB's boundary value problem solver `bvp4c()`.

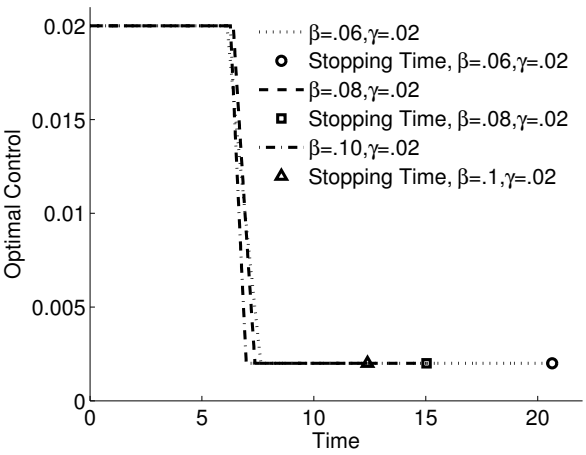


(a) Optimum system cost with respect to the spreading rate, β, for different values of passivity rate, γ.

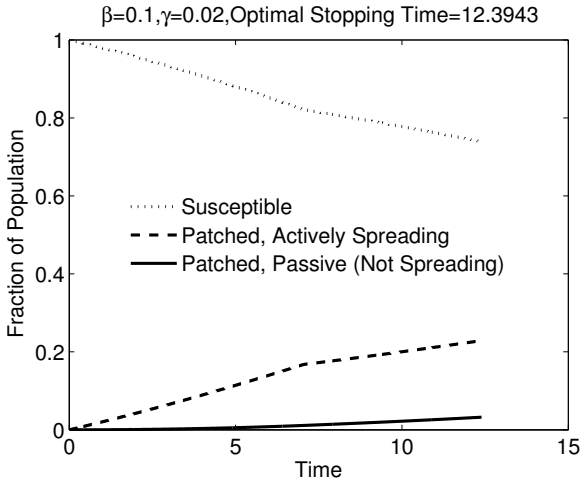


(b) System cost with respect to the spreading rate, β, for different values of passivity rate, γ for heuristic controls. Compare with Fig. (1a) and note the differences in scales of y-axis in the two figures.

Fig. 1: Comparing costs of the optimal and heuristic strategies.



(a) Optimal control with respect to time and optimal stopping time for three different cases.



(b) Fraction of susceptible $s(t)$, patched and actively spreading $a(t)$ and, patched but passive $p(t)$ population with respect to time for $\beta = 0.1$, $\gamma = 0.02$. The optimal stopping time was calculated to be 12.3943.

Fig. 2: Optimal solution and the state variables.

We demonstrate the effectiveness of the optimal control compared to the following *heuristic controls*. Let $u_{h1}(t)$, $u_{h2}(t)$ and $u_{h3}(t)$ be three control signals defined as follows:

$$\begin{aligned} u_{h1} &\equiv u_{min}, \\ u_{h2} &\equiv (u_{min} + u_{max})/2, \\ u_{h3} &\equiv u_{max}. \end{aligned} \tag{9}$$

The stopping time, T, corresponding to these (static) controls are calculated such that the respective cost functionals (given by (1a)) are minimized.

Here, we demonstrate the effectiveness of the optimal control over the heuristic strategies. The optimal system/server costs with respect to spreading rate β—for different passivity rate γ—obtained by applying Pontryagin's Minimum Principle using the *optimal method* described in section III are shown in Fig. (1a). The system costs for the same range of β values obtained by using the three *heuristic methods* in Eq. (9) is shown in Fig. (1b). We note the differences in the scales of Y-axis in both the figures (Figs. (1a) and (1b)) and conclude that the optimal control achieves much lower system costs (in Fig. (1a)) compared to the costs obtained by heuristic controls (in Fig. (1b)) for a given value of spreading rate β.

Fig. (2a) shows the shape of optimal control signal and corresponding optimal stopping time for three sets of parameters.

The control starts with its maximum value, gradually decreases to the minimum value, and then remains constant for the rest of the time. Evolution of the fraction of the susceptible, active and passive population for one set of parameters is shown in Fig. (2b).

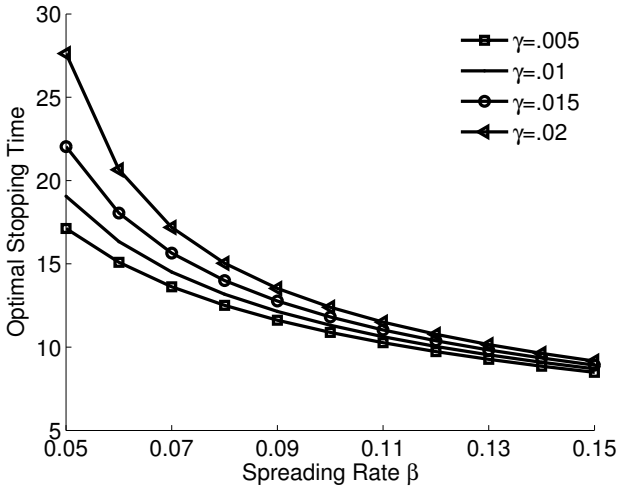


Fig. 3: Optimal stopping time with respect to the spreading rate β for different values of passivity rate γ.

Fig. (3) shows the variation of the optimal stopping time with increasing spreading rate, β, for different passivity rate, γ. It can be seen that optimal stopping time decreases as patch distribution becomes more viral (increasing β) or when nodes switch from active to passive state at a lower rate (decreasing γ) thereby spreading the patch for a longer duration of time. Intuitively, such a behavior will decrease the server workload and hence lower system costs. Same explanation holds for the cost trend seen in Fig. (1a).

V. Conclusion

Devising strategies for spreading security patches to counter the effect of malicious softwares has important practical importance in network management. Previous studies assumed fixed decision horizon. In this paper we have formulated the decision problem of a security patch distribution server (optimal patching intensity and optimal stopping time) as a free terminal time optimal control problem. In this system, in addition to direct patching by the server, patches are also distributed by epidemic contact between susceptible and active nodes. We have shown the effectiveness of the optimal strategy over the heuristic strategies. Also, as the spreading rate of the epidemic contact increases, or the rate of switching from active to passive state among active nodes decreases, the optimal server cost and optimal stopping time decreases, reflecting reduced workload on the server. This work assumes fixed spreading rate β, and passivity rate γ. An interesting avenue of future research is to make these parameters additional control variables of the system.

References

[1] M. Vojnovic and A. Ganesh, "On the Effectiveness of Automatic Patching," in *ACM Work. on Rapid Malcode*. ACM, 2005, pp. 41–50.

[2] S. Shakkottai and R. Srikant, "Peer to Peer Networks for Defense Against Internet Worms," in *Work. on Interdisciplinary Sys. Approach in Performance Evalu. & Design of Comp. & Commu. Sys.* ACM, 2006.

[3] M. Bloem, T. Alpcan, and T. Başar, "Optimal and Robust Epidemic Response for Multiple Networks," *Control Eng. Practice*, vol. 17, no. 5, pp. 525–533, 2009.

[4] M. H. R. Khouzani, S. Sarkar, and E. Altman, "Optimal Dissemination of Security Patches in Mobile Wireless Networks," *IEEE Trans. on Info. Theory*, vol. 58, no. 7, pp. 4714–4732, 2012.

[5] Q. Zhu, X. Yang, L. X. Yang, and C. Zhang, "Optimal Control of Computer Virus Under a Delayed Model," *App. Math. & Comp.*, 2012.

[6] A. Karnik and P. Dayama, "Optimal Control of Information Epidemics," in *IEEE Inter. Conf. on Commu. Sys. & Networks (COMSNETS)*. IEEE, 2012, pp. 1–7.

[7] K. Kandhway and J. Kuri, "Optimal resource allocation over time and degree classes for maximizing information dissemination in social networks," *IEEE/ACM Transactions on Networking*, vol. 24, no. 5, pp. 3204–3217, 2016.

[8] P. Dayama, A. Karnik, and Y. Narahari, "Optimal Incentive Timing Strategies for Product Marketing on Social Networks," *Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2012)*, 2012.

[9] K. Kandhway and J. Kuri, "Campaigning in heterogeneous social networks: Optimal control of si information epidemics," *IEEE/ACM Transactions on Networking*, vol. 24, no. 1, pp. 383–396, 2016.

[10] A. Barrat, M. Barthlemy, and A. Vespignani, *Dynamical Processes on Complex Networks*. Cambridge University Press, 2008.

[11] M. H. R. Khouzani, S. Sarkar, and E. Altman, "Saddle-Point Strategies in Malware Attack," *IEEE J. on Sel. Areas in Commu.*, vol. 30, no. 1, 2012.

[12] M. I. Kamien and N. L. Schwartz, *Dynamic Optimization: the Calculus of Variations and Optimal Control in Economics and Management*. North-Holland Amsterdam, 1991, vol. 1, no. 4.

[13] D. E. Kirk, *Optimal Control Theory: an Introduction*. Courier Dover Publications, 2012.